

## ABSTRACT OF THE DISCLOSURE

A key management device and method which is required for provision of a security service in an EPON vulnerable to security breaches due to characteristics of Ethernet. A session key distribution function is performed in such a manner that, during the process of communication setup between an OLT and an ONU, the OLT multicasts a public key and the ONU receives the public key from the OLT and then distributes a corresponding session key to the OLT. A session key update function is performed in such a manner that an existing session key is updated with a new one through a periodic MPCP general gate message and an ONU report message.